着眼新时代发展 铸信息安全战略之盾

马双荣 绪光 弥纶

中国发展战略学研究会国防战略专业委员会 北京 100000

摘要：[目的/意义]信息技术发展高速迅猛，在人们享受科技带来的便利同时，随之而来的是日益严峻的信息安全形势。这也给我国从网络大国向网络强国迈进提出了新的挑战。[方法/过程]本文分析了当前新时代形势下所面临的非传统安全问题："外联网"威胁网络疆域；大数据技术驱动或引发新的危机；依赖开源谨防关键技术发展受制于人。[结果/结论]基于此，本文对国家信息安全发展给出了一些可供参考的对策性建议。

关键词：**信息安全 外联网 大数据 开源技术**

分类号：D631；TP309

信息技术发展高速迅猛，随之而来的是全球网络空间和信息安全形势愈发严峻，这也给我国从网络大国向网络强国迈进提出了新的挑战。

1 新技术环境下带来非传统安全问题

1.1 "外联网"威胁网络疆域

据外媒报道，2015 年欧美一些科技企业欲发射微、小

卫星系统建立“外联网”，欲实现在世界任何角落的民众都能免费使用互联网，而且在今年中旬，Google 公司的热气球通信系统已经在秘鲁水灾时期成功为该地区提供了网络通信。所谓“外联网”，是指通过布置大量的微小卫星、热气球或无人机等空天飞行器，向地球地面站持续释放传递无线网络信号，使用地面任何电子终端都能进行直接连接上网。[1]然而，人们决不能将此看作是慈善之举。据悉，早在 2011 年就有境外媒体报道，美军将投资七千万美元打造一个“影子互联网”系统，旨在帮助一些国家反对派能够通过这套系统进行无障碍通讯，以避开本国网监和通讯系统封锁，这套系统被命名为“便携式互联网接入器”。而如今“外联网”更像是一个光明正大的“影子互联网”，终将可能成为一些居心叵测政客或组织等的工具。

除此，“外联网”凭借其独有的构建特性，还拥有着抗打击能力强、通信范围广、传输速度快等诸多特点，这或将可能为军方提供有力的通讯保障。此概念在军事上的应用已有成功案例，据悉，驻伊美军曾使用 RQ-7 影子无人机作为移动基站，建立区域空基通信网络，其通讯速度可与 4G 通讯相当，为地面部队随时提供可靠的通讯支持，使其在边远地区作战摆脱了通信难的问题。打赢信息化战争的关键之一就是夺取信息优势，但在“外联网”这全球性高效通信网的面前，网络的物理“疆域”将毫无意义，拥有“外联网”

也就意味着获得信息战的压倒性优势。未来，随着人类社会信息化程度的空前提高，万物互联的智能时代将很快到来，若是 “物联网”也逐步融入“外联网”，将等同于“智能地球”的命脉被少数控制者独揽[2]。

1.2 大数据技术驱动或引发新的危机

大数据，从诞生至今一直是信息技术中的热门词，在商业领域中一直有“大数据时代的数据就是财富”这样的说法。曾有国际研究显示，近几年所产生的数据量约占整个人类文明所产生总数据中的 90%，而且世界所产生的数据规模仍将不断高速增长，不过也正是有了这庞大的数据量，才能使得未来人类各个领域的发展均能产生新时代跨越。此外，大数据技术虽然给我们科技发展和日常生活带来了很多好处，但也有许多隐患值得敲响警钟。今天世界所面临的“大数据”危机，不仅仅是人们耳熟能详的精准营销、隐私泄露等，更多地应该考虑如何能更好地把握国家数据主权。互联网即时共享的特性，使得数据流动难以控制，而对这些数据的掌握与利用，极有可能会影响到国家顶层战略的制定与实施。举个简单的例子，1964 年“照片泄密案”仅一张王进喜的照片，竟泄露出如此多的国家能源资源信息，可见处于“大数据”时代的今天，如果数据主权不能牢牢把控，被肆意“开采”，将有更多重要信息被他人获取[3]。所以如何加强对数据主权的掌控，是当前必须重视的问题。

“记忆数字化”也是当前“大数据”时代的一大特点，互联网作为载体不断记录着人们所产生的一切数据，其数据量以每年约 1.5 倍的速度高速膨胀，可以说，“互联网”已经成为了世界共享的“数字大脑”，只不过我们人类的大脑会不断的遗忘、记忆，但“互联网”会近乎无差别的存储和记忆所有的数据，很少去“遗忘”。这并非益事，网络本身并无对数据的甄别能力，如今不仅数据量庞大，而且其类型繁杂，价值密度极低，导致“大数据”处于混沌的状态，如不严加管控，“大数据”的健康程度将每况愈下，未来也难免会出现数据欺骗等针对大数据的攻击手段[4]。由此可见，应当重视对互联网数据的清理，赋予“数字大脑”遗忘的能力，各国更应携手共建一个中立、有效、安全的国际数据监管体系，共同维护数据秩序，为下一代“机机交互”“智能交互”的新时代互联网打下基础。

除了互联网之外，国防和军事的数据增长也不容小觑，信息化作战更是要面对海量的军事数据，军事大数据时代的来临，已经是新军事变革中各国军方的重要挑战。据外媒报道，美伊战争爆发首日，海量综合保障数据不断冲击着位于卡塔尔和科威特的美军驻伊指挥中枢，由于系统难以承受如此巨大的数据压力而被迫停止运行，导致前线部队失联。由此可知，对海量数据的处理能力已经是当今战争的基本要求，除作战数据外，网络舆情、社交平台信息、自媒体等各类信息数据，

都蕴含着有价值的信息，高效、可靠的开展多领域、跨平台数据挖掘，应是新时代军事变革所必须要解决的问题。据悉，美国为了加强“大数据”这一关键领域的协同作用，不仅组建了“美国大数据研发高级指导小组”，专项负责开展跨部门大数据研发活动，其国防部每年还在军事部门的大数据研发上投入约 2.5 亿美元。可见，国家做好“大数据”发展的顶层设计，引领军民融合共力技术研发与应用，推进多门类跨学科协作，是应对当前“大数据”挑战的正确选择[5]。

1.3　依赖开源谨防关键技术发展受制于人

“开源”源自计算机领域，在互联网初期，一部分程序员倡导共享精神，发布其开发的软件源代码供大家使用，这类软件就被称为开源软件。而今新能源汽车技术开源、安全技术开源、云计算开源、工业自动化平台开源等等，如雨后春笋，这看似是低成本经济快速发展的最佳途径，但其实不然。全球化市场早有一种说法，三流企业卖产品，二流企业卖技术，一流企业推标准。这里，技术开源正是被当作一种隐性的标准推行，是一种新的市场竞争模式。不过回眸 2008 年微软 Windows“系统黑屏事件”，到 2016 年三星“电池门”事件强制永久禁用特定型号手机，再到不久前被披露的，多款惠普电脑音频驱动内置隐藏键盘记录器，会自动记录用户键入信息等，我们可以看到很多企业目的并不纯正，其系统技术内部很可能留有多个后门，简单的“拿来主义”，终将

会给信息安全带来严重威胁。若这一幕幕非传统安全事件在其他工业制造、信息安全等关键领域上演，其后果将难以想象，这决不是危言耸听。2016 年 9 月，网络上流传着特斯拉电动汽车被入侵的视频，仅通过远程攻击，入侵者即可轻易遥控被入侵车辆。无独有偶，2017 年 9 月 13 日，美国国土安全部发表声明，要求美国联邦机构禁止使用卡巴斯基任何软件，可见美国政府或已担忧俄罗斯可能通过其入侵该系统。遵循他国主流标准，购买现有廉价技术、商品，或许能够节约大量的研发资金和人力物力，只需要享受技术带来的发展便利，但这并不是长远发展的明智之举。[6]今后这种“开源”现象将会在更多的行业领域出现，更多的所谓国际标准将被推行，但我们必须清楚认识“天下没有免费的午餐”，这并不仅是专利能否使用的主动权被掌握在他人的手里，更是会产生发展的技术断层，失去在众多领域的主导权，尤其在国防和军事上，这更是应当重视的大问题，否则在信息化战争中将带来难以估量的损失。

2　新形势下信息安全发展的对策建议

一是加强顶层设计，完善在新兴领域的法律法规建设。现如今各国网络安全顶层设计都在逐步完善，但在新兴的领域仍存在着许多空缺，如今信息化技术标准、规则、协议更多的是民间组织、企业所制定，而这些条款的制定更多地考虑是开放、便捷、经济效益等，并未从政治的角度、国家安

全的角度来考虑，如果我们只是被动地接受执行，就相当于接受了其中所存在的各类漏洞与隐患，可谓是后患无穷。美国作为网络技术最发达的国家，始终没有在网络安全立法上掉以轻心，目前已经出台了数十部法律来加强网络安全保护，尽管如此，美国在网络安全立法方面依然不敢松懈。所以，迎接新时代的变革和挑战，制定和完善全面的信息安全法律法规是当务之急，任重道远。

二是研发颠覆性技术，占领信息安全制高点。颠覆性技术是一种能够对已有传统或主流技术途径产生颠覆性效果和作用的先进技术，可能是完全创新的技术，也可能是基于现有技术的跨学科、跨领域的创新型应用。我国应当大力支持研发颠覆性技术，抢先占领战略制高点，大胆创新鼓励交叉学科研究，运用颠覆性技术，以特殊的方式代替传统技术，占领多领域主流技术阵地，抵消信息技术与发达国家的差距。尤其在国防和军事领域，颠覆性技术一直在不断影响着战争形态的改变，推动着军事变革新时代的发展。

三是支持军民融合型科技企业，深入开展信息安全战略合作。我国的科技创新水平与日俱增，国内的科技型企业在世界上已经有了长足进步。然而，从信息安全的角度考虑，加强对军民融合型科技企业的支持，不应仅仅停留在经济、政策上的扶持，国家更应推动其建立安全战略上的合作。“棱镜门”事件显示，硅谷主要电信传播公司与国家安全局依法

共享信息，使得国家能够通过分析数据来更好地甄别外界对美国的威胁。如今科技企业掌握着更多涉及到公共安全、信息安全的关键数据和安全技术，例如，推特作为世界最大的社交平台之一，其平台内舆论导向将会影响世界大量人的思想状态。所以，政府与企业建立良好的合作关系，将更有利于建立完善的国家安全体系。

四是普及信息安全知识，加强全民信息安全教育。信息安全不仅是国家的责任，更是每一位公民都应尽的责任，随着信息化程度越来越高，每一个人都应懂得信息安全知识，增强信息安全意识，这就要从教育着手。应当统筹现有国家信息安全网络教育活动，更加深入的开展全民信息安全教育，一是应将信息安全教育纳入义务教育的范畴，从娃娃抓起，树立一代代人的信息安全观；二是建立健全成人信息安全技能培训认证，为信息安全建设储备必要人才；三是设立专职信息安全岗位，带动人才培养。从而以教育为抓手，全面提高国家整体信息安全水平。

参考文献：

[1] 马双荣,叶奇佳. 该如何面对大数据来袭[N]. 解放军报，2014-04-14(007).
[2] 何峰,张琪. 重视网信安全 共建网信安全[N]. 中国远洋海运报，2017-10-27(B01).
[3] 杜雁云. 大数据时代国家数据主权问题研究[J]. 国际观察,2016(03):1-14.
[4] 沈国麟. 大数据时代的数据主权和国家数据战略[J]. 南京社会科学,2014(06):113-119,127.
[5] 沈雪石,张爱军,赵海洋. 颠覆性技术对武器装备发展的影响及思考[J]. 国防科技,2015,36(03):18-22.
[6] 常斐. 让网络安全意识深入人心[N]. 成都日报，2017-09-25(004).

作者贡献说明：

马双荣：撰写论文全文初稿；

绪光：设计本文研究思路，修改论文；

弥纶：研究框架设计，论文撰写。

Developing the Shield of Information Security Strategy In the New Era

Ma Shuangrong Xu Guang Mi Guan

National Defense Strategy Specialized Committee, Chinese Association of Development Strategy Studies, Beijing 100000

Abstract: [Purpose/significance] The information technology develops rapidly. While people enjoy the convenience brought by the technology, the information security situation is increasingly serious. It also presents a new challenge for China's development from a big network power to a strong network power. **[Method/process]** This paper analyzed the non-traditional security issues under the current situation of the new era, for example, the threat of extranet towards the network field, the crisis probably caused by the big-data-driven technology, the limitation of developing key technologies caused by relying on foreign open source technologies. **[Result/conclusion]** This paper gives some suggestions for the development of the national information security.

Keywords: information security extranet big data open source technology

收稿日期：2017-11-17 修回日期：2017-12-06 本文责任编辑：唐果媛